

On isotopisms and strong isotopisms of commutative presemifields

G. Marino* and O. Polverino*

Abstract

In this paper we prove that the $P(q, \ell)$ (q odd prime power and $\ell > 1$ odd) commutative semifields constructed by Bierbrauer in [1] are isotopic to some commutative presemifields constructed by Budaghyan and Helleseeth in [2]. Also, we show that they are strongly isotopic if and only if $q \equiv 1 \pmod{4}$. Consequently, for each $q \equiv -1 \pmod{4}$ there exist isotopic commutative presemifields of order $q^{2\ell}$ ($\ell > 1$ odd) defining CCZ-inequivalent planar DO polynomials.

1 Introduction

A finite *semifield* \mathbb{S} is a finite binary algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity of multiplication. If \mathbb{S} satisfies all axioms for a semifield except the existence of an identity element for the multiplication, then we call it a *presemifield*. The additive group of a presemifield is an elementary abelian p -group, for some prime p called the *characteristic* of \mathbb{S} .

The definition of nuclei and center of a semifield can be found, for instance, in [8, Sec. 5.9]. A finite semifield is a vector space over its nuclei and its center. Two presemifields, say $\mathbb{S}_1 = (\mathbb{S}_1, +, \bullet)$ and $\mathbb{S}_2 = (\mathbb{S}_2, +, \star)$ of characteristic p , are said to be *isotopic* if there exist three \mathbb{F}_p -linear permutations M, N, L from \mathbb{S}_1 to \mathbb{S}_2 such that

$$M(x) \star N(y) = L(x \bullet y)$$

for all $x, y \in \mathbb{S}_1$. The triple (M, N, L) is an *isotopism* between \mathbb{S}_1 and \mathbb{S}_2 . They are *strongly isotopic* if we can choose $M = N$. From any presemifield, one can naturally construct a semifield which is isotopic to it (see [11]). The sizes of the nuclei as well as the size of the center of a semifield are invariant under isotopy. The isotopism relation between semifields arises from the isomorphism relation between the projective planes coordinatized by them (*semifield planes*). For a recent overview on the theory of finite semifields see Chapter [12] in the collected work [7].

*This work was supported by the Research Project of MIUR (Italian Office for University and Research) “Geometrie su Campi di Galois, piani di traslazione e geometrie di incidenza”.

Commutative presemifields in odd characteristic can be equivalently described by planar DO polynomials [6]. A *Dembowski–Ostrom (DO) polynomial* $f \in \mathbb{F}_q[x]$ ($q = p^e$) is a polynomial of the shape $f(x) = \sum_{i,j=0}^{e-1} a_{ij}x^{p^i+p^j}$, whereas a polynomial $f \in \mathbb{F}_q[x]$ is *planar* or *perfect nonlinear* (PN for short) if, for each $a \in \mathbb{F}_q^*$, the mapping $x \mapsto f(x+a) - f(x) - f(a)$ is bijective. If $f(x) \in \mathbb{F}_q[x]$ is a planar DO polynomial, then $\mathbb{S}_f = (\mathbb{F}_q, +, \star)$ is a commutative presemifield where $x \star y = f(x+y) - f(x) - f(y)$. Conversely, if $\mathbb{S} = (\mathbb{F}_q, +, \star)$ is a commutative presemifield of odd order, then the polynomial $f(x) = \frac{1}{2}(x \star x)$ is a planar DO polynomial and $\mathbb{S} = \mathbb{S}_f$.

Two functions F and F' from \mathbb{F}_{p^n} to itself are called *Carlet–Charpin–Zinoviev equivalent (CCZ–equivalent)* if for some affine permutation \mathcal{L} of $\mathbb{F}_{p^n}^2$ the image of the graph of F is the graph of F' , that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) | x \in \mathbb{F}_{p^n}\}$ and $G_{F'} = \{(x, F'(x)) | x \in \mathbb{F}_{p^n}\}$ (see [4]). By [2, Sec. 4], two planar DO polynomials are CCZ–equivalent if and only if the corresponding presemifields are strongly isotopic. In [5], it has been proven that two presemifields of order p^n , with p prime and n odd integer, are strongly isotopic if and only if they are isotopic. Whereas, for $n = 6$ and $p = 3$, Zhou in [16], by using MAGMA computations, has shown that the presemifields constructed in [13] and [2] are isotopic but not strongly isotopic. In [1], the author proved that the two families of commutative presemifields constructed in [2] are contained, up to isotopy, into a unique family of presemifields, and we refer to it as the family \mathcal{BHB} . Also in [1], the author generalized the commutative semifields constructed in [13] (\mathcal{LMPTB} semifields) proving that each \mathcal{LMPTB} semifield is not isotopic to any previously known semifield with the possible exception of \mathcal{BHB} presemifields.

In this paper we study the isotopy and strong isotopy relations involving the above commutative presemifields, proving that the \mathcal{LMPTB} semifields are contained, up to isotopy, in the family of \mathcal{BHB} presemifields. Precisely, we show that an \mathcal{LMPTB} semifield of order $q^{2\ell}$ (q odd and $\ell > 1$ odd) is isotopic to a \mathcal{BHB} presemifield, and that they are strongly isotopic if and if $q \equiv 1 \pmod{4}$. This yields that, for planar DO functions from $\mathbb{F}_{q^{2\ell}}$ to itself, when $q \equiv -1 \pmod{4}$ and $\ell > 1$ odd, the isotopy relation is strictly more general than CCZ–equivalence.

2 Preliminary results

If $\mathbb{S} = (\mathbb{S}, +, \bullet)$ is a presemifield, then $\mathbb{S}^* = (\mathbb{S}, +, \bullet^*)$, where $x \bullet^* y = y \bullet x$ is a presemifield as well, and it is called the *dual* of \mathbb{S} . If \mathbb{S} be a presemifield of order p^n , then we may assume that $\mathbb{S} = (\mathbb{F}_{p^n}, +, \bullet)$, where $x \bullet y = F(x, y) = \sum_{i,j=0}^{n-1} a_{ij}x^{p^i}y^{p^j}$, with $a_{ij} \in \mathbb{F}_{p^n}$. The set

$$S = \{\varphi_y : x \in \mathbb{F}_{p^n} \mapsto F(x, y) \in \mathbb{F}_{p^n} \mid y \in \mathbb{F}_{p^n}\} \subseteq \mathbb{V} = \text{End}(\mathbb{F}_{p^n}, \mathbb{F}_p)$$

is the spread set associated with \mathbb{S} and

$$S^* = \{\varphi^x : y \in \mathbb{F}_{p^n} \mapsto F(x, y) \in \mathbb{F}_{p^n} \mid x \in \mathbb{F}_{p^n}\} \subseteq \mathbb{V} = \text{End}(\mathbb{F}_{p^n}, \mathbb{F}_p)$$

is the spread set associated with \mathbb{S}^* . Both S and S^* are subgroups of order p^n of the additive group of \mathbb{V} and each nonzero element of S and S^* is invertible.

For each $x \in \mathbb{F}_{p^n}$, the *conjugate* $\bar{\varphi}$ of the element $\varphi(x) = \sum_{i=0}^{n-1} \beta_i x^{p^i}$ of \mathbb{V} is defined by $\bar{\varphi}(x) = \sum_{i=0}^{n-1} \beta_i^{p^{n-i}} x^{p^{n-i}}$. The map

$$T : \varphi \in \mathbb{V} \mapsto \bar{\varphi} \in V$$

is an \mathbb{F}_p -linear permutation of \mathbb{V} . Straightforward computations show that

$$\overline{\varphi \circ \psi} = \bar{\psi} \circ \bar{\varphi} \quad \overline{\varphi^{-1}} = (\bar{\varphi})^{-1}. \quad (1)$$

The algebraic structure $\mathbb{S}^t = (\mathbb{F}_{p^n}, +, \bullet^t)$, where $x \bullet^t y = \overline{\varphi_y}(x)$, is a presemifield and it is called the *transpose* of \mathbb{S} (see e.g. [13, Lemma 2]). The set $S^t = \{\overline{\varphi_y} \mid y \in \mathbb{F}_{p^n}\}$ is the spread set associated with \mathbb{S}^t .

In what follows we want to point out the relationship between spread sets associated with two isotopic presemifields.

Proposition 2.1. *Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \bullet)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields and let $S_1 = \{\varphi_y : x \mapsto x \bullet y \mid y \in \mathbb{F}_{p^n}\}$ and $S_2 = \{\varphi'_y : x \mapsto x \star y \mid y \in \mathbb{F}_{p^n}\}$ be the corresponding spread sets. Then \mathbb{S}_1 and \mathbb{S}_2 are isotopic under the isotopism (M, N, L) if and only if $S_2 = LS_1M^{-1} = \{L \circ \varphi_y \circ M^{-1} \mid y \in \mathbb{F}_{p^n}\}$.*

Proof. The necessary condition can be easily proven. Indeed if (M, N, L) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 , then $L(\varphi_y(x)) = \varphi'_{N(y)}(M(x))$ for each $x, y \in \mathbb{F}_{p^n}$. Hence, $\varphi'_{N(y)} = L \circ \varphi_y \circ M^{-1}$ for each $y \in \mathbb{F}_{p^n}$ and the statement follows taking into account that $S_2 = \{\varphi'_{N(y)} \mid y \in \mathbb{F}_{p^n}\}$.

Conversely, let $S_2 = \{L \circ \varphi_y \circ M^{-1} \mid y \in \mathbb{F}_{p^n}\}$, where M and L are two \mathbb{F}_p -linear permutations of \mathbb{F}_{p^n} . It is easy to see that the map N , sending each element $y \in \mathbb{F}_{p^n}$ to the unique element $z \in \mathbb{F}_{p^n}$ such that $\varphi'_z = L \circ \varphi_y \circ M^{-1}$ (where $\varphi'_z \in S_2$), is an \mathbb{F}_p -linear permutations of \mathbb{F}_{p^n} . Hence, for each $x, y \in \mathbb{F}_{p^n}$ we get $\varphi'_{N(y)}(x) = L(\varphi_y(M^{-1}(x)))$, i.e. $x \star N(y) = L(M^{-1}(x) \bullet y)$ and putting $x' = M^{-1}(x)$ we have the assertion. \square

Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$ be a presemifield, where $x \star y = F(x, y) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i} y^{p^j}$, with $a_{ij} \in \mathbb{F}_{p^n}$, and let S and S^* be the spread sets associated with \mathbb{S} and \mathbb{S}^* , respectively.

The middle (respectively, right) nucleus of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{N}_m(\mathbb{S})$ (respectively, $\mathcal{N}_r(\mathbb{S})$) contained in $\mathbb{V} = \text{End}(\mathbb{F}_{p^n}, \mathbb{F}_p)$ such that $S\mathcal{N}_m(\mathbb{S}) \subseteq S^1$ (respectively, $\mathcal{N}_r(S)S \subseteq S$), whereas the left nucleus of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{N}_l(\mathbb{S})$ contained in \mathbb{V} such that $\mathcal{N}_l(\mathbb{S})S^* \subseteq S^*$ (see [15, Thm. 2.1] and [14]).

Also, if \mathbb{F}_q is a subfield of \mathbb{F}_{p^n} and $F(x, y)$ is a q -polynomial with respect to the variable x , i.e. $S \subset \text{End}(\mathbb{F}_{p^n}, \mathbb{F}_q)$, then $F_q = \{t_\lambda : x \in \mathbb{F}_{p^n} \mapsto \lambda x \in \mathbb{F}_{p^n} \mid \lambda \in \mathbb{F}_q\} \subset \mathcal{N}_l(\mathbb{S})$ ([14]).

If (M, N, L) is an isotopism between two presemifields \mathbb{S}_1 and \mathbb{S}_2 , we have that $\mathcal{N}_r(S_2) = L\mathcal{N}_r(S_1)L^{-1}$, $\mathcal{N}_m(S_2) = M\mathcal{N}_m(S_1)M^{-1}$ and $\mathcal{N}_l(S_2) = L\mathcal{N}_l(S_1)L^{-1}$ (see e.g. [9] and [14]).

From these results we can prove

¹By juxtaposition we will always denote the composition of maps that will be read from right to left.

Theorem 2.2. *If (M, N, L) is an isotopism between two presemifields \mathbb{S}_1 and \mathbb{S}_2 of order p^n , whose associated spread sets S_1 and S_2 are contained in $\text{End}(\mathbb{F}_{p^n}, \mathbb{F}_q)$ (\mathbb{F}_q a subfield of \mathbb{F}_{p^n}), then L and M are \mathbb{F}_q -semilinear maps of \mathbb{F}_{p^n} with the same companion automorphism.*

Proof. Since $S_1, S_2 \subset \text{End}(\mathbb{F}_{p^n}, \mathbb{F}_q)$, by the previous arguments we have that

$$F_q = \{t_\lambda : x \in \mathbb{F}_{p^n} \mapsto \lambda x \in \mathbb{F}_{p^n} | \lambda \in \mathbb{F}_q\} \subset \mathcal{N}_l(\mathbb{S}_1) \cap \mathcal{N}_l(\mathbb{S}_2).$$

Also $\mathcal{N}_l(S_2) = L\mathcal{N}_l(S_1)L^{-1}$. Then $L^{-1}F_qL \subset \mathcal{N}_l(\mathbb{S}_2)$, and since a field contains a unique subfield of given order, it follows $L^{-1}F_qL = F_q$. Since the map $t_\lambda \mapsto L^{-1}t_\lambda L$ is an automorphism of the field of maps F_q , there exists $i \in \{0, \dots, n-1\}$ such that $L^{-1}t_\lambda L = t_{\lambda^{p^i}}$ for each $\lambda \in \mathbb{F}_q$, i.e. L is an \mathbb{F}_q -semilinear map of \mathbb{F}_{p^n} with companion automorphism $\sigma(x) = x^{p^i}$. Also, by Proposition 2.1, $LS_1M^{-1} = S_2$, and hence M is an \mathbb{F}_q -semilinear map of \mathbb{F}_{p^n} as well, with the same companion automorphism σ . \square

Finally, since the dual and the transpose operations are invariant under isotopy [11], it makes sense to ask which is the isotopism involving the duals and the transposes of two isotopic presemifields. We have the following result.

Proposition 2.3. *Let \mathbb{S}_1 and \mathbb{S}_2 be two presemifields. Then*

- i) (M, N, L) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if (N, M, L) is an isotopism between the dual presemifields \mathbb{S}_1^* and \mathbb{S}_2^* ;*
- ii) (M, N, L) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if $(\overline{L}^{-1}, N, \overline{M}^{-1})$ is an isotopism between the transpose presemifields \mathbb{S}_1^t and \mathbb{S}_2^t ;*
- iii) (M, N, L) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if $(N, \overline{L}^{-1}, \overline{M}^{-1})$ is an isotopism between \mathbb{S}_1^{t*} and \mathbb{S}_2^{t*} .*

Proof. Statement *i)* easily follows from the definition of the dual operation, whereas *iii)* follows from *i)* and *ii)*.

Let us prove *ii)*. Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \bullet)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$ and let $S_1 = \{\varphi_y | y \in \mathbb{F}_{p^n}\}$ and $S_2 = \{\varphi'_y | y \in \mathbb{F}_{p^n}\}$ be the corresponding spread sets. By the previous arguments the corresponding transpose presemifields are $\mathbb{S}_1^t = (\mathbb{F}_{p^n}, +, \bullet^t)$ and $\mathbb{S}_2^t = (\mathbb{F}_{p^n}, +, \star^t)$, where $x \bullet^t y = \overline{\varphi_y}(x)$ and $x \star^t y = \overline{\varphi'_y}(x)$, respectively. The triple (M, N, L) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if $L \circ \varphi_y = \varphi'_{N(y)} \circ M$ for each $y \in \mathbb{F}_{p^n}$. By (1), $\overline{\varphi_y} \circ \overline{L} = \overline{M} \circ \overline{\varphi'_{N(y)}}$ for each $y \in \mathbb{F}_{p^n}$ and hence

$$\overline{L}(x) \bullet^t y = \overline{M}(x \star^t N(y))$$

for each $x, y \in \mathbb{F}_{p^n}$. By (1), this is equivalent to $\overline{M}^{-1}(z \bullet^t y) = \overline{L}^{-1}(z) \star^t N(y)$ for each $z, y \in \mathbb{F}_{p^n}$. The assertion follows. \square

Finally, by *iii*) of Proposition 2.3 and by Proposition 2.1 we immediately get the following result.

Corollary 2.4. *Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \bullet)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields and let S_1^{t*} and S_2^{t*} be the spread sets associated with the presemifields \mathbb{S}_1^{t*} and \mathbb{S}_2^{t*} , respectively. Then \mathbb{S}_1 and \mathbb{S}_2 are strongly isotopic if and only if there exists an \mathbb{F}_p -linear permutation H of \mathbb{F}_{p^n} such that $S_2^{t*} = HS_1^{t*}\overline{H}$.*

3 \mathcal{BHB} and \mathcal{LMPTB} commutative presemifields

The \mathcal{BHB} presemifields and the \mathcal{LMPTB} semifields presented in [1] can be described as follows.

\mathcal{BHB} $B(p, m, s, \beta)$ presemifields [2], [1]: $(\mathbb{F}_{p^{2m}}, +, \star)$, p odd prime and $m > 1$, with

$$x \star y = xy^{p^m} + x^{p^m}y + [\beta(xy^{p^s} + x^{p^s}y) + \beta^{p^m}(xy^{p^s} + x^{p^s}y)^{p^m}]\omega, \quad (2)$$

where $0 < s < 2m$, ω is an element of $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ with $\omega^{p^m} = -\omega$ and the following conditions are satisfied:

$$\beta \in \mathbb{F}_{p^{2m}}^* : \beta^{\frac{p^{2m}-1}{(p^m+1, p^s+1)}} \neq 1 \quad \text{and} \quad \nexists a \in \mathbb{F}_{p^{2m}}^* : a + a^{p^m} = a + a^{p^s} = 0. \quad (3)$$

\mathcal{LMPTB} $P(q, \ell)$ semifields [13], [1]: $(\mathbb{F}_{q^{2\ell}}, +, *)$, q odd prime power and $\ell = 2k+1 > 1$ odd, with

$$x * y = \frac{1}{2}(xy + x^{q^\ell}y^{q^\ell}) + \frac{1}{4}G(xy^{q^2} + x^{q^2}y),$$

where $G(x) = \sum_{i=1}^k (-1)^i (x - x^{q^\ell})^{q^{2i}} + \sum_{j=1}^{k-1} (-1)^{k+j} (x - x^{q^\ell})^{q^{2j+1}}$.

In order to prove our results, we start by further investigating Multiplication (2) and Conditions (3). Set $h := \gcd(m, s)$, then $m = h\ell$ and $s = hd$, where ℓ and d are two positive integers such that $0 < d < 2\ell$ and $\gcd(\ell, d) = 1$. Putting $q = p^h$, then $\omega \in \mathbb{F}_{q^{2\ell}} \setminus \mathbb{F}_{q^\ell}$ such that $\omega^{q^\ell} = -\omega$ and the \mathcal{BHB} presemifields $B(p, m, s, \beta) = (\mathbb{F}_{q^{2\ell}}, +, \star)$ will be denoted by $\overline{B}(q, \ell, d, \beta)$. Moreover, Multiplication (2) and Conditions (3) can be rewritten as

$$x \star y = xy^{q^\ell} + x^{q^\ell}y + [\beta(xy^{q^d} + x^{q^d}y) + \beta^{q^\ell}(xy^{q^d} + x^{q^d}y)^{q^\ell}]\omega,$$

where

$$\beta \in \mathbb{F}_{q^{2\ell}}^* : \beta^{\frac{q^{2\ell}-1}{(q^\ell+1, q^d+1)}} \neq 1, \quad (4)$$

and

$$\nexists a \in \mathbb{F}_{q^{2\ell}}^* : a + a^{q^\ell} = a + a^{q^d} = 0. \quad (5)$$

We get the following preliminary result.

Lemma 3.1. *i) Condition (5) is fulfilled if and only if $\ell + d$ is odd.*

ii) If Condition (5) is fulfilled, then an element $\beta \in \mathbb{F}_{q^{2\ell}}^$ satisfies Condition (4) if and only if β is a nonsquare of $\mathbb{F}_{q^{2\ell}}$.*

Proof. *i)* The sufficient condition can be easily proven. Indeed, since $\gcd(\ell, d) = 1$ then ℓ and d cannot be both even integers. Moreover, if ℓ and d were both odd, then each element $a \in \mathbb{F}_{q^2}$ such that $a^q = -a$ would be a solution of $x^{q^\ell} = x^{q^d} = -x$, contradicting our assumption. On the other hand, suppose that $\ell + d$ is odd, then $\gcd(2\ell, \ell + d) = \gcd(\ell, d) = 1$. Hence, if there exists an element $a \in \mathbb{F}_{q^{2\ell}}^*$ such that $a^{q^\ell} + a = a^{q^d} + a = 0$, then a satisfies the equation $x^{q^{\ell+d}-1} = 1$, which admits $\gcd(q^{2\ell} - 1, q^{\ell+d} - 1) = q^{\gcd(2\ell, \ell+d)} - 1 = q - 1$ solutions. It follows that $a \in \mathbb{F}_q^*$, a contradiction.

ii) We first suppose ℓ is odd and d is even and prove that $\gcd(q^\ell + 1, q^d + 1) = 2$. If $q \equiv 1 \pmod{4}$, then $q^\ell + 1 \equiv q^d + 1 \equiv 2 \pmod{4}$. On the other hand, if $q \equiv 3 \pmod{4}$, since ℓ is odd and d is even, $q^\ell + 1 \equiv 0 \pmod{4}$ and $q^d + 1 \equiv 2 \pmod{4}$. So in both cases 2 is the maximum power of 2 dividing $\gcd(q^\ell + 1, q^d + 1)$. Now suppose that p' is an odd prime such that $p' | (q^\ell + 1)$ and $p' | (q^d + 1)$. Hence $q^\ell \equiv -1 \pmod{p'}$ and $q^d \equiv -1 \pmod{p'}$. Since $\gcd(\ell, d) = 1$, then $1 = a\ell + bd$, with a an odd integer. From the previous congruences it follows that $q = q^{a\ell+bd} \equiv (-1)^a(-1)^b \pmod{p'} \equiv (-1)^{b+1} \pmod{p'}$ and since d is even, we have $q^d \equiv 1 \pmod{p'}$, a contradiction.

If ℓ is even and d is odd, arguing as in the previous case we obtain the assertion. \square

Remark 3.2. By Lemma 3.1, the algebraic structure $\overline{B}(q, \ell, d, \beta)$ is a presemifield if and only if $\ell + d$ is odd and β is a nonsquare in $\mathbb{F}_{q^{2\ell}}$.

In [1], the author proved that the semifields $P(q, \ell)$ are not isotopic to any previously known commutative semifield with the possible exception of \mathcal{BHB} presemifields. In what follows, using the notation introduced in this section, we study the isotopy relation involving the families of presemifields $P(q, \ell)$ and $\overline{B}(q, \ell, d, \beta)$ and we prove that a $P(q, \ell)$ semifield of order $q^{2\ell}$, with $q = p^e$ an odd prime power and $\ell > 1$ an odd integer, is isotopic to a $\overline{B}(q, \ell, 2, \beta)$ presemifield for a suitable choice of β .

4 The isotopism issue

By [10], there is a canonical bijection between commutative and symplectic presemifields. Precisely, if \mathbb{S} is a commutative presemifield, then \mathbb{S}^{t*} is a symplectic presemifield. Moreover, by *iii)* of Proposition 2.3, two commutative presemifields are isotopic if and only if the corresponding symplectic presemifields are isotopic as well. So, in the next, we will prove that the symplectic presemifield $P(q, \ell)^{t*}$ is isotopic to a symplectic presemifield $\overline{B}(q, \ell, 2, \beta)^{t*}$.

The symplectic version of $P(q, \ell)$ semifields

From [1, Sec. 3], the symplectic presemifield arising from the commutative semifield $P(q, \ell)$, q an odd prime power and $\ell = 2k + 1$ an odd integer, is $P(q, \ell)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \bullet)$ with multiplication given by

$$x \bullet y = \frac{y + y^{q^\ell}}{2}x + \frac{1}{4}(y - y^{q^\ell} + \alpha_y + \beta_y + \gamma_y)x^{q^2} + \frac{1}{4}(y - y^{q^\ell} - \alpha_y - \beta_y - \gamma_y)x^{q^{2\ell-2}},$$

where $\alpha_y = \sum_{i=1}^{\ell-1} (-1)^{i+1} y^{q^{2i}}$, $\beta_y = \sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{2j+1}}$ and $\gamma_y = \sum_{t=k+1}^{\ell-1} (-1)^{k+t} y^{q^{2t+1}}$. Setting $g(y) := \alpha_y + \beta_y + \gamma_y$ and

$$f(y) := \frac{1}{4}(y - y^{q^\ell} + g(y)),$$

direct computations show that

$$f(y)^{q^{2\ell-2}} = \frac{1}{4}(y - y^{q^\ell} - g(y)). \quad (6)$$

Indeed, reducing modulo $y^{q^{2\ell}} - y$, we have

$$4f(y)^{q^{2\ell-2}} = y^{q^{2\ell-2}} - y^{q^{\ell-2}} + \sum_{i=1}^{\ell-1} (-1)^{i+1} y^{q^{2(i-1)}} + \sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{2j-1}} + \sum_{t=k+1}^{\ell-1} (-1)^{k+t} y^{q^{2t-1}}$$

and setting $i' = i - 1$, $j' = j - 1$, $t' = t - 1$, we get

$$\begin{aligned} 4f(y)^{q^{2\ell-2}} &= y - y^{q^\ell} + \sum_{i'=1}^{\ell-1} (-1)^{i'} y^{q^{2i'}} + \sum_{j'=0}^{k-1} (-1)^{k+j'+1} y^{q^{2j'+1}} + \sum_{t'=k+1}^{\ell-1} (-1)^{k+t'} y^{q^{2t'+1}} \\ &= y - y^{q^\ell} - (\alpha_y + \beta_y + \gamma_y). \end{aligned}$$

Hence

$$x \bullet y = \frac{y + y^{q^\ell}}{2}x + f(y)x^{q^2} + f(y)^{q^{2\ell-2}}x^{q^{2\ell-2}}. \quad (7)$$

Let $\eta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\eta^q = -\eta$. Since q and $\ell = 2k + 1$ are odd integers, the map $\phi : \gamma \in \mathbb{F}_{q^\ell} \mapsto \gamma + \gamma^{q^2} \in \mathbb{F}_{q^\ell}$ is invertible and

$$\phi^{-1} : z \in \mathbb{F}_{q^\ell} \mapsto \frac{1}{2} \left(\sum_{i=0}^k (-1)^i z^{q^{2i}} + \sum_{j=0}^{k-1} (-1)^{k+j+1} z^{q^{2j+1}} \right) \in \mathbb{F}_{q^\ell}.$$

Taking into account that $\{1, \eta\}$ is an \mathbb{F}_{q^ℓ} -basis of $\mathbb{F}_{q^{2\ell}}$ and that ϕ is an invertible map, it follows that any element $y \in \mathbb{F}_{q^{2\ell}}$ can be uniquely written as

$$y = A + (B^{q^2} + B)\eta,$$

with $A, B \in \mathbb{F}_{q^\ell}$. Also

$$A = \frac{y + y^{q^\ell}}{2} \quad (8)$$

and

$$B^{q^2} + B = \frac{y - y^{q^\ell}}{2\eta}$$

Direct computations show that

$$\begin{aligned} B &= \phi^{-1} \left(\frac{y - y^{q^\ell}}{2\eta} \right) = \frac{1}{2} \left(\sum_{i=0}^k (-1)^i \frac{(y - y^{q^\ell})^{q^{2i}}}{2\eta} + \sum_{j=0}^{k-1} (-1)^{k+j+1} \frac{(y - y^{q^\ell})^{q^{2j+1}}}{-2\eta} \right) \\ &= \frac{1}{4\eta} \left(y - y^{q^\ell} + \sum_{i=1}^k (-1)^i y^{q^{2i}} - \sum_{i=1}^k (-1)^i y^{q^{\ell+2i}} - \sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{2j+1}} + \sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{\ell+2j+1}} \right). \end{aligned} \quad (9)$$

Putting $2t + 1 := \ell + 2i$, i.e. $i = t - k$, we have

$$\sum_{i=1}^k (-1)^i y^{q^{\ell+2i}} = \sum_{t=k+1}^{\ell-1} (-1)^{t-k} y^{q^{2t+1}} = \sum_{t=k+1}^{\ell-1} (-1)^{t+k} y^{q^{2t+1}}$$

and putting $2v := \ell + 2j + 1$, i.e. $j = v - k - 1$, we have

$$\sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{\ell+2j+1}} = \sum_{v=k+1}^{\ell-1} (-1)^v y^{q^{2v}}.$$

Hence, substituting the last two equalities in Equation (9), we get

$$B = \frac{1}{4\eta} \left(y - y^{q^\ell} + \sum_{i=1}^{\ell-1} (-1)^i y^{q^{2i}} - \sum_{j=0}^{k-1} (-1)^{k+j+1} y^{q^{2j+1}} - \sum_{t=k+1}^{\ell-1} (-1)^{t+k} y^{q^{2t+1}} \right) = \frac{1}{4\eta} (y - y^{q^\ell} - \alpha_y - \beta_y - \gamma_y)$$

and, taking (6) into account, this yields $f(y) = B^{q^2} \eta$. Hence, from (7), (8) and the last equality, we get the following result.

Proposition 4.1. *The symplectic presemifield $P(q, \ell)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \bullet)$ arising from the commutative semifield $P(q, \ell)$ has multiplication*

$$x \bullet y = Ax + B^{q^2} \eta x^{q^2} + B \eta x^{q^{2\ell-2}},$$

where η is a given element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\eta^q = -\eta$ and $y = A + (B^{q^2} + B)\eta$, $A, B \in \mathbb{F}_{q^\ell}$. \square

The symplectic version of $\overline{B}(q, \ell, d, \beta)$ -presemifields

Let q be an odd prime power, ℓ and d be integers such that $0 < d < 2\ell$, $\ell + d$ is odd and $\gcd(\ell, d) = 1$. Then a commutative $\overline{B}(q, \ell, d, \beta)$ -presemifield is of type $(\mathbb{F}_{q^{2\ell}}, +, \star)$, where

$$x \star y = xy^{q^\ell} + x^{q^\ell}y + [\beta(xy^{q^d} + x^{q^d}y) + \beta^{q^\ell}(xy^{q^d} + x^{q^d}y)^{q^\ell}]\omega,$$

with β a nonsquare in $\mathbb{F}_{q^{2\ell}}$ and $\omega^{q^\ell} = -\omega$ (see Remark 3.2). By using [13, Lemmas 1, 2], the transpose semifield $\overline{B}^t(q, \ell, d, \beta) = (\mathbb{F}_{q^{2\ell}}, +, \star^t)$ of $\overline{B}(q, \ell, d, \beta)$ is defined by

$$x \star^t y = (x + x^{q^\ell})y^{q^\ell} + \beta^{q^{2\ell-d}}\omega^{q^{2\ell-d}}(x^{q^{2\ell-d}} - x^{q^{\ell-d}})y^{q^{2\ell-d}} + \beta\omega(x - x^{q^\ell})y^{q^d}.$$

Hence $\overline{B}^{t*}(q, \ell, d, \beta) = (\mathbb{F}_{q^{2\ell}}, +, \star^{t*})$, where

$$x \star^{t*} y = (y + y^{q^\ell})x^{q^\ell} + \beta^{q^{2\ell-d}}\omega^{q^{2\ell-d}}(y^{q^{2\ell-d}} - y^{q^{\ell-d}})x^{q^{2\ell-d}} + \beta\omega(y - y^{q^\ell})x^{q^d}.$$

Since $\{1, \omega\}$ is an \mathbb{F}_{q^ℓ} -basis of $\mathbb{F}_{q^{2\ell}}$, putting $y = A + B\omega$, with $A, B \in \mathbb{F}_{q^\ell}$ and recalling that $\omega^{q^\ell} = -\omega$, and hence $\omega^2 = \sigma \in \mathbb{F}_{q^\ell}^*$, we get

Proposition 4.2. *The symplectic presemifield $\overline{B}(q, \ell, d, \beta)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \star')$ arising from the commutative semifield $\overline{B}(q, \ell, d, \beta)$ has multiplication*

$$x \star' y = 2Ax^{q^\ell} + 2\sigma^{q^{2\ell-d}}\beta^{q^{2\ell-d}}B^{q^{2\ell-d}}x^{q^{2\ell-d}} + 2\sigma\beta Bx^{q^d}, \quad (10)$$

where β is a nonsquare in $\mathbb{F}_{q^{2\ell}}$ and $y = A + B\omega$ with $A, B \in \mathbb{F}_{q^\ell}$, σ is a nonsquare in \mathbb{F}_{q^ℓ} and $\omega^2 = \sigma$. \square

Remark 4.3. Note that if σ and σ' are two nonsquare elements of \mathbb{F}_{q^ℓ} , then $\sigma' = t\sigma$, where t is a nonzero square in \mathbb{F}_{q^ℓ} . So, replacing β by $t\beta$ in (10), we may substitute σ with σ' . It follows that, when ℓ is **odd**, in order to study, up to isotopy, the \mathcal{BHB} presemifields we may suppose wlg that σ is a nonsquare in \mathbb{F}_q and hence $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

The isotopism theorem

Let start by proving the following

Theorem 4.4. *Let q be an odd prime power, let ℓ and d be odd and even integers, respectively, such that $0 < d < 2\ell$ and $\gcd(\ell, d) = 1$. The symplectic presemifield $\overline{B}(q, \ell, d, \beta)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \star')$, whose multiplication is given in (10), is isotopic to a presemifield $(\mathbb{F}_{q^{2\ell}}, +, \star'')$ whose multiplication is given by*

$$x \star'' y = 2 \left(Ax + \sigma B\omega \frac{\beta}{\xi^{q^\ell}} x^{q^d} + \sigma B^{q^{2\ell-d}} \omega \frac{\beta^{q^{2\ell-d}}}{\xi^{q^\ell}} x^{q^{2\ell-d}} \right),$$

where $y = A + B\omega$ with $A, B \in \mathbb{F}_{q^\ell}$, $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\omega^2 = \sigma \in \mathbb{F}_q^*$, and ξ is an element of $\mathbb{F}_{q^{2\ell}}$ such that $\xi^{q^{\ell+d}-1} = \beta^{1-q^\ell}$ and $\xi^{q^\ell+1} = \sigma$.

Proof. By Proposition 4.2 and Remark 4.3, the spread set associated with the symplectic pre-semifield $\overline{B}(q, \ell, d, \beta)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \star')$ is

$$S = \{\varphi_y = \varphi_{A,B} : x \mapsto 2Ax^{q^\ell} + 2\sigma\beta^{q^{2\ell-d}}B^{q^{2\ell-d}}x^{q^{2\ell-d}} + 2\sigma\beta Bx^{q^d} \mid y = A + B\omega, A, B \in \mathbb{F}_{q^\ell}\},$$

where β and σ are nonsquares in $\mathbb{F}_{q^{2\ell}}$ and \mathbb{F}_q , respectively.

Since $\gcd(q^{2\ell} - 1, q^{\ell+d} - 1) = q - 1$ and $(\beta^{1-q^\ell})^{\frac{q^{2\ell}-1}{q-1}} = 1$, the following equation

$$x^{q^{\ell+d}-1} = \beta^{1-q^\ell}. \quad (11)$$

admits $q-1$ distinct solutions in $\mathbb{F}_{q^{2\ell}}$. Moreover, if ξ and $\bar{\xi}$ satisfy (11), then $\xi/\bar{\xi} \in \mathbb{F}_q^*$. Also, if ξ is a solution of (11), then $\xi^{q^\ell+1}$ is a solution of $x^{q^{\ell+d}-1} = 1$ and since $\gcd(q^{2\ell}-1, q^{\ell+d}-1) = q-1$, we get $\xi^{q^\ell+1} \in \mathbb{F}_q^*$. Moreover, taking into account that β is a nonsquare in $\mathbb{F}_{q^{2\ell}}$, it follows that $\xi^{q^\ell+1}$ is a nonsquare in \mathbb{F}_q . Indeed if $(\xi^{q^\ell+1})^{\frac{q-1}{2}} = 1$, then $(\frac{1}{\beta})^{\frac{q^{2\ell}-1}{2}} = (\xi^{q^{\ell+d}-1})^{\frac{q^\ell+1}{2}} = (\xi^{q^\ell+1})^{\frac{q^{\ell+d}-1}{2}} = 1$, a contradiction. Hence the set $\{\xi^{q^\ell+1} \mid \xi \text{ is a solution of (11)}\} \subset \mathbb{F}_q$ is the set of nonsquares in \mathbb{F}_q . This means that we can choose $\xi \in \mathbb{F}_{q^{2\ell}}$, satisfying (11) and such that

$$\xi^{q^\ell+1} = \sigma = \omega^2. \quad (12)$$

Now, consider the invertible maps of $\mathbb{F}_{q^{2\ell}}$

$$\psi : x \mapsto \frac{\omega}{\xi}x + x^{q^\ell} \quad \text{and} \quad \phi : x \mapsto x - \frac{\omega}{\xi q^\ell}x^{q^\ell}$$

and note that

$$\psi^{-1} : x \mapsto \frac{1}{2}\left(\frac{\omega}{\xi q^\ell}x + x^{q^\ell}\right) \quad \text{and} \quad \psi^{-1}(\phi(x)^{q^\ell}) = x.$$

Since ψ and ϕ are linear maps over \mathbb{F}_{q^ℓ} , for each $x \in \mathbb{F}_{q^{2\ell}}$ we have

$$\begin{aligned} \psi^{-1} \circ \varphi_{A,B} \circ \phi(x) &= 2(\psi^{-1}(A(\phi(x))^{q^\ell} + \sigma\beta^{q^{2\ell-d}}B^{q^{2\ell-d}}(\phi(x))^{q^{2\ell-d}} + \sigma\beta B(\phi(x))^{q^d})) \\ &= 2(Ax + \sigma B^{q^{2\ell-d}}\psi^{-1}(f(x)) + \sigma B\psi^{-1}(g(x))), \end{aligned} \quad (13)$$

where $f(x) = (\beta\phi(x))^{q^{2\ell-d}}$ and $g(x) = \beta(\phi(x))^{q^d}$.

Then, taking into account that $\omega^q = -\omega$, direct computations show that

$$\psi^{-1}(f(x)) = \frac{1}{2}f_1x^{q^{\ell-d}} + \frac{1}{2}f_2x^{q^{2\ell-d}},$$

with $f_1 = -\frac{\omega^2}{\xi^{q^\ell+q^{\ell-d}}} \beta^{q^{2\ell-d}} + \beta^{q^{\ell-d}}$ and $f_2 = \frac{\omega}{\xi q^\ell} \beta^{q^{2\ell-d}} + \frac{\omega}{\xi q^{2\ell-d}} \beta^{q^{\ell-d}}$.

By (11), we get $\beta^{q^\ell} = \frac{\beta\xi}{\xi^{q^\ell+1}}$ and elevating to the $q^{2\ell-d}$ -th power we have $\beta^{q^{\ell-d}} = \beta^{q^{2\ell-d}} \xi^{q^\ell(q^{\ell-d}-1)}$.

From (12) it follows $\beta^{q^{\ell-d}} = \beta^{q^{2\ell-d}} \left(\frac{\omega^2}{\xi}\right)^{(q^{\ell-d}-1)} = (\beta^{q^{2\ell-d}} \frac{\omega^2}{\xi^{q^{\ell-d}}}) \frac{\xi}{\omega^2} = \beta^{q^{2\ell-d}} \frac{\omega^2}{\xi^{q^{\ell-d}+q^\ell}}$; hence $f_1 = 0$.

Also, $f_2 = \omega(\frac{\beta^{q^{\ell-d}}}{\xi^{q^{2\ell-d}}} + \frac{\beta^{q^{2\ell-d}}}{\xi^{q^\ell}})$ and by (11) we have $f_2 = 2\omega\frac{\beta^{q^{2\ell-d}}}{\xi^{q^\ell}}$. Hence, $\psi^{-1}(f(x)) = \omega\frac{\beta^{q^{2\ell-d}}}{\xi^{q^\ell}}x^{q^{2\ell-d}}$, and using similar arguments we have $\psi^{-1}(g(x)) = \omega\frac{\beta}{\xi^{q^\ell}}x^{q^d}$. Then, by (13), we get

$$\psi^{-1} \circ \varphi_{A,B} \circ \phi(x) = 2Ax + 2\sigma B\omega\frac{\beta}{\xi^{q^\ell}}x^{q^d} + 2\sigma B^{q^{2\ell-d}}\omega\frac{\beta^{q^{2\ell-d}}}{\xi^{q^\ell}}x^{q^{2\ell-d}}.$$

Hence,

$$\psi^{-1} \circ \varphi_y \circ \phi(x) = x \star'' y,$$

i.e.

$$\phi(x) \star' y = \psi(x \star'' y). \quad (14)$$

This means that (ϕ, id, ψ) is an isotopism between the two presemifields. The theorem is proven. \square

Theorem 4.5. *Each \mathcal{LMPTB} semifield is isotopic to a \mathcal{BHB} presemifield.*

Proof. By Proposition 4.1 the symplectic presemifield $P(q, \ell)^{t*} = (\mathbb{F}_{q^{2\ell}}, +, \bullet)$, q odd and $\ell > 1$ odd, arising from the commutative semifield $P(q, \ell)$ has multiplication

$$x \bullet y = Ax + B^{q^2}\eta x^{q^2} + B\eta x^{q^{2\ell-2}},$$

where $\eta^q = -\eta$ and $y = A + (B^{q^2} + B)\eta$ with $A, B \in \mathbb{F}_{q^\ell}$.

Put $d = 2$ in Theorem 4.4 and choose $\beta = \bar{\beta}$ as a nonsquare in $\mathbb{F}_{q^{2\ell}}$ belonging to \mathbb{F}_{q^2} such that $\bar{\beta}^{q+1} = \frac{1}{\sigma}$. Then $\bar{\beta}^{-1}$ is a solution of Equation (11) and since $\bar{\beta}^{q^\ell+1} = \bar{\beta}^{q+1} = \frac{1}{\sigma}$, we can fix $\xi = \bar{\beta}^{-1}$. By Theorem 4.4 the symplectic presemifield $\overline{B}(q, \ell, 2, \bar{\beta})^{t*}$ is isotopic to the presemifield $(\mathbb{F}_{q^{2\ell}}, +, \star'')$ whose multiplication is given by

$$x \star'' y = 2Ax + 2B\omega x^{q^2} + 2B^{q^{2\ell-2}}\omega x^{q^{2\ell-2}},$$

where $\omega^q = -\omega$ and $y = A + B\omega$ with $A, B \in \mathbb{F}_{q^\ell}$. Let $\omega = \alpha\eta$ and note that $\alpha \in \mathbb{F}_q^*$.

Let $h : y = A + B\omega \in \mathbb{F}_{q^{2\ell}} \mapsto 2A + 2(B^{q^{2\ell-2}} + B)\omega \in \mathbb{F}_{q^{2\ell}}$. Since q and ℓ are odd, h is an invertible \mathbb{F}_q -linear map of $\mathbb{F}_{q^{2\ell}}$. Also, since $h(y) = h(A + B\omega) = 2A + 2((\alpha B^{q^{2\ell-2}})^{q^2} + (\alpha B^{q^{2\ell-2}}))\eta$ we have

$$x \bullet h(y) = x \star'' y$$

for each $x, y \in \mathbb{F}_{q^\ell}$, hence by (14) we get

$$\phi(x) \star' h^{-1}(z) = \psi(x \bullet z)$$

for each $x, z \in \mathbb{F}_{q^\ell}$. Then (ϕ, h^{-1}, ψ) is an isotopism between $P(q, \ell)^{t*}$ and $\overline{B}(q, \ell, 2, \bar{\beta})^{t*}$. The theorem is proven. \square

By Theorems 4.4, 4.5 and by *iii*) of Proposition 2.3 we can state the following result.

Corollary 4.6. *The triple $(\bar{\psi}^{-1}, \phi, \bar{h})$ is an isotopism between the commutative semifield $P(q, \ell)$ and the presemifield $\bar{B}(q, \ell, 2, \bar{\beta})$, where $\bar{\beta}$ is a nonsquare in \mathbb{F}_{q^2} .*

Remark 4.7. Note that, since $\bar{\psi}^{-1} \neq \phi$, the above isotopism is not a strong isotopism.

5 Strong Isotopism

In this section we will prove that the isotopic presemifields $P(q, \ell)$ and $\bar{B}(q, \ell, 2, \bar{\beta})$ of Corollary 4.6, are strongly isotopic if and only if $q \equiv 1 \pmod{4}$. Let us start by proving the following.

Theorem 5.1. *If $q \equiv 1 \pmod{4}$, then the commutative presemifields $P(q, \ell)$ and $\bar{B}(q, \ell, 2, \bar{\beta})$ of Corollary 4.6 are strongly isotopic.*

Proof. By Corollary 2.4, the two involved presemifields are strongly isotopic if and only if there exists an invertible \mathbb{F}_p -linear map H of $\mathbb{F}_{q^{2\ell}}$, such that $HS_1\bar{H} = S_2$, where S_1 and S_2 are the spread sets associated with $P(q, \ell)^{t*}$ and $\bar{B}(q, \ell, 2, \bar{\beta})^{t*}$, respectively. By the proof of Theorem 4.5 and by Proposition 2.1, we have that $\psi S_1 \phi^{-1} = S_2$, where

$$\psi : x \mapsto \omega \bar{\beta} x + x^{q^\ell} \quad \text{and} \quad \phi^{-1} : x \mapsto \frac{1}{2}(x + \omega \bar{\beta}^q x^{q^\ell}),$$

with the choices of $\bar{\beta}$ and ξ as in Theorem 4.5. Recall that $\omega \bar{\beta} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\bar{\beta}$ is a nonsquare in $\mathbb{F}_{q^{2\ell}}$, $\omega^2 = \sigma \in \mathbb{F}_q$ and $\bar{\beta}^{q+1} = \frac{1}{\sigma}$.

Let $\rho = 2\omega \bar{\beta}$ and note that $\bar{\phi}^{-1}(\rho x) = \psi(x)$, i.e. $\bar{\phi}^{-1} \circ t_\rho = \psi$, where $t_\rho(x) = \rho x$.

Since $q \equiv 1 \pmod{4}$ and $\omega^{q-1} = -1$, we have that ω is a nonsquare in \mathbb{F}_{q^2} , and hence $\rho = 2\omega \bar{\beta}$ is a square in \mathbb{F}_{q^2} . Let $b \in \mathbb{F}_{q^2}$ such that $b^2 = \rho$ and let $H(x) = \bar{\phi}^{-1}(bx)$, i.e. $H = \bar{\phi}^{-1} \circ t_b$ is an invertible \mathbb{F}_p -linear map of $\mathbb{F}_{q^{2\ell}}$. Then, by (1), we get

$$HS_1\bar{H} = (\bar{\phi}^{-1} \circ t_b)S_1(t_b \circ \phi^{-1}).$$

Since the elements of S_1 are \mathbb{F}_{q^2} -linear maps of $\mathbb{F}_{q^{2\ell}}$ and $b \in \mathbb{F}_{q^2}$ we have

$$HS_1\bar{H} = (\bar{\phi}^{-1} \circ t_{b^2})S_1\phi^{-1} = (\bar{\phi}^{-1} \circ t_\rho)S_1\phi^{-1} = \psi S_1\phi^{-1} = S_2.$$

This proves the theorem. □

Finally, we can prove

Theorem 5.2. *If $q \equiv -1 \pmod{4}$, then the commutative presemifields $P(q, \ell)$ and $\bar{B}(q, \ell, 2, \bar{\beta})$ of Corollary 4.6 are not strongly isotopic.*

Proof. By way of contradiction, suppose that the two involved presemifields are strongly isotopic. Then by Corollary 2.4, there exists an invertible \mathbb{F}_p -linear map H of $\mathbb{F}_{q^{2\ell}}$, $q = p^h$, such that

$HS_1\overline{H} = S_2$, where S_1 and S_2 are the spread sets associated with \mathbb{S}_1^{t*} and \mathbb{S}_2^{t*} , respectively. In particular

$$S_1 = \{\varphi_{A,B} : x \mapsto Ax + B^{q^2}\eta x^{q^2} + B\eta x^{q^{2\ell-2}} \mid y = A + (B^{q^2} + B)\eta, y \in \mathbb{F}_{q^{2\ell}}\}.$$

By Theorem 4.5, $\psi S_1 \phi^{-1} = S_2$, hence $\psi^{-1}HS_1\overline{H}\phi = S_1$, where

$$\psi^{-1} : x \mapsto \frac{1}{2}(\omega\bar{\beta}^q x + x^{q^\ell}) \quad \phi : x \mapsto x - \omega\bar{\beta}^q x^{q^\ell}$$

and $\psi^{-1} = \frac{1}{2}\omega\bar{\beta}^q\overline{\phi}$. It follows that

$$\delta GS_1\overline{G} = S_1, \tag{15}$$

where $\delta = \frac{1}{2}\omega\bar{\beta}^q \in \mathbb{F}_{q^2}$ and $G = \overline{\phi}H$. Since the elements of S_1 are \mathbb{F}_{q^2} -linear maps of $\mathbb{F}_{q^{2\ell}}$, by Theorem 2.2 and Proposition 2.1, we have that G is an invertible \mathbb{F}_{q^2} -semilinear map of $\mathbb{F}_{q^{2\ell}}$, with companion automorphism $\sigma = p^e$.

Let

$$G(x) = \sum_{i=0}^{\ell-1} a_i x^{p^{2hi+e}} = \sum_{i=0}^{\ell-1} a_i x^{\sigma q^{2i}},$$

then

$$\overline{G}(x) = \sum_{i=0}^{\ell-1} a_i^{p^{2\ell h-2hi-e}} x^{p^{2\ell h-2hi-e}} = \sum_{i=0}^{\ell-1} a_i^{\sigma^{-1}q^{2\ell-2i}} x^{\sigma^{-1}q^{2\ell-2i}}.$$

By (15), the map $\delta(G \circ \varphi_{A,0} \circ \overline{G})$ belongs to S_1 for each $A \in \mathbb{F}_{q^\ell}$. Then there exist $A', B' \in \mathbb{F}_{q^\ell}$ such that $\delta(G(A(\overline{G}(x)))) = \varphi_{A',B'}(x)$ for each $x \in \mathbb{F}_{q^{2\ell}}$.

Since

$$\delta(G(A(\overline{G}(x)))) = \delta\left(\sum_{j=0}^{\ell-1} \sum_{i=0}^{\ell-1} A^{\sigma q^{2j}} a_j a_i^{q^{2(\ell-i+j)}} x^{q^{2(\ell-i+j)}}\right) = A'x + B'^{q^2}\eta x^{q^2} + B'\eta x^{q^{2\ell-2}},$$

reducing the above polynomial identity modulo $x^{q^{2\ell}} - x$ and by comparing the coefficients of first degree, we get

$$\delta(A^\sigma a_0^2 + A^{\sigma q^2} a_1^2 + \cdots + A^{\sigma q^{2\ell-2}} a_{\ell-1}^2) = A' \in \mathbb{F}_{q^\ell}$$

for each $A \in \mathbb{F}_{q^\ell}$, i.e.

$$A^\sigma(\delta a_0^2 - \delta^q a_0^{2q^\ell}) + A^{\sigma q^2}(\delta a_1^2 - \delta^q a_1^{2q^\ell}) + \cdots + A^{\sigma q^{2\ell-2}}(\delta a_{\ell-1}^2 - \delta^q a_{\ell-1}^{2q^\ell}) = 0$$

for each $A \in \mathbb{F}_{q^\ell}$. This is equivalent to

$$(\bar{\beta}^q a_0^2 + \bar{\beta} a_0^{2q^\ell})x + (\bar{\beta}^q a_1^2 + \bar{\beta} a_1^{2q^\ell})x^{q^2} + \cdots + (\bar{\beta}^q a_{\ell-1}^2 + \bar{\beta} a_{\ell-1}^{2q^\ell})x^{q^{2\ell-2}} = 0$$

for each $x \in \mathbb{F}_{q^\ell}$. Reducing the above polynomial identity over \mathbb{F}_{q^ℓ} modulo $x^{q^\ell} - x$, we get

$$\bar{\beta}^q a_i^2 + \bar{\beta} a_i^{2q^\ell} = 0$$

for each $i \in \{0, 1, \dots, \ell - 1\}$. If $a_i \neq 0$, then a_i is a solution of

$$x^{2q^\ell - 2} = -\bar{\beta}^{q-1}.$$

However, when $q \equiv -1 \pmod{4}$, the last equation admits no solution in $\mathbb{F}_{q^{2\ell}}$. Hence the unique \mathbb{F}_{q^2} -semilinear map satisfying (15) is the zero one, a contradiction. \square

References

- [1] J. BIERBRAUER: Commutative semifields from projection mappings, *Designs, Codes, Cryptogr.*, **61** (2011), 187–196. DOI 10.1007/s10623-010-9447-z.
- [2] L. BUDAGHYAN, T. HELLESETH: New Perfect Nonlinear Multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p , *Lecture Notes in comput. Sci.*, vol. 5203, SETA (2008), 403–414.
- [3] L. BUDAGHYAN, T. HELLESETH: New commutative semifields defined by PN multinomials, *Cryptogr. Commun.*, **3**, no. 1, (2011), 1–16.
- [4] C. CARLET, P. CHARPIN, V. ZINOVIEV: Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptography*, **15**, no. 2, (1998), 125–156.
- [5] R.S. COULTER, M. HENDERSON: Commutative presemifields and semifields, *Adv. Math.*, **217** (2008), 282–304.
- [6] R.S. COULTER, R.W. MATTHEWS: Planar functions and planes of Lenz–Barlotti clas II, *Des. Codes Cryptography*, **10** (1997), 167–184.
- [7] J. DE BEULE, L. STORME (Editors): *Current research topics in Galois Geometry*, NOVA Academic Publishers, to appear.
- [8] N. L. JOHNSON, V. JHA, M. BILIOTTI: *Handbook of Finite Translation Planes*, Pure and Applied Mathematics, Taylor Books, 2007.
- [9] N.L. JOHNSON, G. MARINO, O. POLVERINO, R. TROMBETTI: Semifields of order q^6 with left nucleus \mathbb{F}_{q^3} and center \mathbb{F}_q , *Finite Fields Appl.*, **14** n. 2 (2008), 456–469.
- [10] W.M. KANTOR: Commutative semifields and symplectic spreads, *J. Algebra*, **270** (2003), 96–114.
- [11] D.E. KNUTH: Finite semifields and projective planes, *J. Algebra*, **2** (1965), 182–217.

- [12] M. LAVRAUW, O. POLVERINO: Finite semifields. Chapter in *Current research topics in Galois Geometry* (J. De Be Storme, Eds.), NOVA Academic Publishers, to appear.
- [13] G. LUNARDON, G. MARINO, O. POLVERINO, R. TROMBETTI: Symplectic Semifield Spreads of $PG(5, q)$ and the Veronese Surface, *Ricerche di Matematica*, **60** No.1 (2011), 125–142. DOI 10.1007/s11587-010-0098-1.
- [14] G. MARINO, O. POLVERINO: On the nuclei of a finite semifield, submitted.
- [15] G. MARINO, O. POLVERINO, R. TROMBETTI: Towards the classification of rank 2 semifields 6-dimensional over their center, *Designs, Codes, Cryptogr.*, **61** No.1 (2011), 11–29. DOI 10.1007/s10623-010-9436-2.
- [16] Y. ZHOU: A Note on the Isotopism of Commutative Semifields, submitted.

G. Marino and O. Polverino
 Dip. di Matematica
 Seconda Università degli Studi di Napoli
 I–81100 Caserta, Italy
giuseppe.marino@unina2.it, olga.polverino@unina2.it